AUSA Matthew Weinberg

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

v.

KENDEL ANTHONY MELBOURNE,

Defendant.

24 MAG 1876

SEALED COMPLAINT

24 Mag. _____

SOUTHERN DISTRICT OF NEW YORK, ss.:

BRYAN DEMBERGER, being duly sworn, deposes and says that he is a Special Agent with the Federal Bureau of Investigation ("FBI"), and charges as follows:

COUNT ONE
(Conspiracy to Commit Computer Intrusion)

1. From at least in or about April 2021 through at least in or about February 2022, in the Southern District of New York and elsewhere, KENDEL ANTHONY MELBOURNE, the defendant, and others known and unknown, willfully and knowingly combined, conspired, confederated, and agreed together and with each other to commit a computer intrusion, in violation of Title 18, United States Code, Section 1030(a)(5)(A).

2. It was a part and an object of the conspiracy that KENDEL ANTHONY MELBOURNE, the defendant, and others known and unknown, knowingly would and did cause the transmission of a program, information, code, and command, and as a result of such conduct, intentionally would and did cause damage without authorization to a protected computer, which caused loss to one and more persons during any one-year period aggregating at least $5,000 in value, to wit, MELBOURNE and others agreed to engage in a scheme to send fraudulent requests to change login credentials for social media accounts from the Southern District of New York, which caused password reset links to be sent by email to co-conspirators without the true subscribers' knowledge or consent, and which caused a loss of at least $5,000 to a social media company during a one-year period, in violation of Title 18, United States Code, Sections 1030(a)(5)(A), 1030(c)(4)(A)(i)(I), and 1030(c)(4)(B)(i).

Overt Act

3. In furtherance of the conspiracy and to effect the illegal object thereof, the following overt acts, among others, were committed in the Southern District of New York and elsewhere:

a. On or about June 13, 2021, KENDEL ANTHONY MELBOURNE, the defendant, submitted a change password request for an online social networking account that did

not belong to MELBOURNE ("Account-1"). The email address for Account-1 was reset on or about June 14, 2021.

(Title 18, United States Code, Section 371.)

COUNT TWO
(Computer Intrusion)

4. From at least in or about April 2021 through at least in or about February 2022, in the Southern District of New York and elsewhere, KENDEL ANTHONY MELBOURNE, the defendant, knowingly caused the transmission of a program, information, code, and command, and as a result of such conduct, intentionally caused damage without authorization to a protected computer, which caused loss to one and more persons during any one-year period aggregating at least $5,000 in value, to wit, MELBOURNE and others engaged in a scheme to send fraudulent requests to change login credentials for social media accounts from the Southern District of New York, which caused password reset links to be sent by email to co-conspirators without the true subscribers' knowledge or consent, and which caused a loss of at least $5,000 to a social media company during a one-year period.

(Title 18, United States Code, Sections 1030(a)(5)(A), (c)(4)(A)(i)(I), (c)(4)(B)(i), and 2.)

5. I am a Special Agent with the Federal Bureau of Investigation ("FBI"), assigned to a cybercrime squad. I have received training and have participated in investigations of computer intrusions, Internet-based financial crimes, and money laundering, among other crimes. I am familiar with the facts and circumstances set forth below from my examination of reports and records, interviews I have conducted, and conversations with other law enforcement officers and other individuals. Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements and conversations of others are reported herein, they are reported in substance and in part, unless noted otherwise.

6. Based on my training and experience and communications with representatives of a social media company that operates multiple social networking services (the "Social Media Company"), I know, among other things, the following:

a. The Social Media Company is a United States company, headquartered in California, that owns and operates two free-access social networking services ("Service-1" and "Service-2"). Service-1 and Service-2 are accessible through their respective websites and mobile applications and allow subscribers to acquire and use their accounts to share messages, multimedia, and other information with other users and the general public.

b. The Social Media Company collects basic contact and personal identifying information from users during the Service-1 and Service-2 account registration processes and thereafter. This information, which can later be changed by the user, may include the user's full name, date of birth, gender, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, credit card or bank account number, and other personal identifiers. The Social Media Company keeps records of changes made to this information. A Service-1

subscriber accesses his or her account by entering the email address or phone number that the subscriber provided during the registration process and a password. Similarly, a Service-2 subscriber accesses his or her account by entering the email address, username, or phone number provided during the registration process and a password. Each Service-2 account is identified by a unique username chosen by the user. Users of Service-2 can change their usernames whenever they choose, but no two users can have the same usernames at the same time.

c. The Social Media Company also collects and retains information about how each user accesses and uses Service-1 and Service-2. This includes information about the Internet Protocol ("IP") addresses used to create and use an account, unique identifiers and other information about devices and web browsers used to access an account, and session times and durations.

d. The Social Media Company hires outside contractors, including those employed by a certain company ("Company-1"), in addition to the Social Media Company's own employees.

e. The Social Media Company operates an internal process through which personnel and contractors of the Social Media Company can request customer support on behalf of family and friends, including relatives and friends who need help resetting their login credentials for Service-1 and/or Service-2 (the "Change Password Process").

7. Based on my review of information and data relating to approximately 120 Service-1 and Service-2 accounts provided by the Social Media Company pursuant to grand jury subpoenas and court orders, I have learned the following, among other things:

a. Between at least in or about April 2021 and at least in or about February 2022, a group of contractors from Company-1 (each individually a "Company-1 Contractor," and collectively the "Company-1 Contractors"), who were assigned to the Social Media Company's office in Manhattan, New York, used the Change Password Process fraudulently to request email address resets for approximately 120 Service-1 and Service-2 subscriber accounts (collectively, the "Accounts"). Of those 120 fraudulent requests for the Change Password Process, approximately 93 were successful. Of the 93 successful requests, approximately 90 related to Service-2 accounts.

b. Of those approximately 120 email address resets for the Accounts, approximately 34 of them were submitted by a particular Company-1 Contractor named KENDEL ANTHONY MELBOURNE, the defendant. Specifically, between in or about April 2021 and in or about July 2021, MELBOURNE submitted approximately 34 requests for the Change Password Process, of which approximately 23 requests were successful. In each case, MELBOURNE indicated that he was submitting the request on behalf of a friend or relative. Furthermore, in most cases, MELBOURNE falsely indicated that the Accounts for which he was requesting resets had been "hacked," "disabled," or otherwise inaccessible. In some cases, MELBOURNE asked that the Account be transferred to another account with a different username and email address, by providing the existing email address for the Account at issue and a new email address to which a password reset link should be sent.

8. Based on my review of cryptocurrency records obtained from a California-based cryptocurrency exchange ("Exchange-1") and a Cayman Islands-based cryptocurrency exchange ("Exchange-2"), I believe that KENDEL ANTHONY MELBOURNE, the defendant, was a manager of a Service-1 and Service-2 account takeover scheme that involved other Company-1 Contractors as co-conspirators. In particular, Exchange-1 and Exchange-2 records show that after numerous instances of a successful reset of an Account's email address through the Change Password Process, a cryptocurrency account registered to MELBOURNE at Exchange-1 ("MELBOURNE's Exchange-1 Account") received Bitcoin ("BTC") transfers from an account registered to a co-conspirator ("CC-1") at Exchange-2 ("CC-1's Exchange-2 Account"). In cases where the successful request for the Change Password Process had been submitted by a co-conspirator other than MELBOURNE, MELBOURNE transferred a portion of the cryptocurrency payment that he received from CC-1 to the co-conspirator who submitted the successful request. The following are examples of some the transactional activity:

a. On or about June 13, 2021, MELBOURNE submitted a Change Password Process request for Account-1. The email address for Account-1 was reset on or about June 14, 2021. That same day, MELBOURNE's Exchange-1 Account received approximately 0.0492 BTC, equivalent to approximately $1,976,[1] from CC-1's Exchange-2 Account.

b. Another co-conspirator ("CC-2") – also a Company-1 Contractor – submitted a Change Password Process request for Account-2 on or about July 2, 2021, and for Account-3 on or about July 5, 2021. Both of these Accounts were reset on or about July 7, 2021. On or about July 7, 2021, MELBOURNE's Exchange-1 Account received two payments totaling 0.1139 BTC, equivalent to approximately $3,960, from CC-1's Exchange-2 Account. MELBOURNE's Exchange-1 Account then sent approximately 0.0577 BTC, equivalent to approximately $2,001, to CC-2.

c. Another co-conspirator ("CC-3") – also a Company-1 Contractor – submitted a Change Password Process request for Account-4 on or about July 19, 2021. The request was approved on or about July 20, 2021. On or about that same day – that is, July 20, 2021 – MELBOURNE's Exchange-1 Account received approximately 0.0662 BTC, equivalent to approximately $1,977, from CC-1's Exchange-2 Account, and transferred approximately 0.0570 BTC, equivalent to approximately $1,690, to CC-3.

d. On or about December 3, 2021, the email address for Account-5 was reset based on a Change Password Process request submitted by another co-conspirator ("CC-4") – also a Company-1 Contractor. That same day, MELBOURNE's Exchange-1 Account received approximately 0.0357 BTC, equivalent to approximately $1,967, from CC-1's Exchange-2 Account, and sent approximately 0.0218 BTC, equivalent to approximately $1,200, to CC-4.

e. On or about December 4, 2021, the email address for Account-6 was reset based on a Change Password Process request submitted by CC-4. That same day, MELBOURNE's Exchange-1 Account received approximately 0.0401 BTC, equivalent to

[1] The BTC to United States Dollar conversions contained herein are based on the exchange rate at the time of the transaction, as indicated in records that I have reviewed from Exchange-1 and Exchange-2.

approximately $1,972, from CC-1's Exchange-2 Account, and sent approximately 0.0205 BTC, equivalent to approximately $1,000, to CC-4.

f. On or about January 13, 2022, the email addresses for three accounts, specifically Account-7, Account-8, and Account-9, were reset based on Change Password Process requests submitted by CC-4. On or about January 13, 2022, MELBOURNE's Exchange-1 Account received approximately 0.2345 BTC, equivalent to approximately $10,031, from CC-1's Exchange-2 Account, and sent approximately 0.1528 BTC, equivalent to approximately $6,546, to CC-4. A day later, on or about January 14, 2022, MELBOURNE's Exchange-1 Account received an additional approximately 0.1507 BTC, equivalent to approximately $6,471, from CC-1's Exchange-2 Account, and sent approximately 0.0942, equivalent to approximately $3,972, to CC-4.

g. In total, CC-1 transferred a total of at least approximately $220,840 to MELBOURNE. In turn, MELBOURNE transferred approximately $66,472.35 to CC-4 and a total of approximately $40,732 to seven other co-conspirators.

9. Based on the pattern and timing of payments from CC-1 to KENDEL ANTHONY MELBOURNE, the defendant, and from MELBOURNE to the other co-conspirators who submitted fraudulent requests for the Change Password Process, I believe that MELBOURNE was paid by CC-1 to submit, and worked with others to submit, fraudulent Change Password Process requests in exchange for payment for each successfully reset Account.

10. I have interviewed three subscribers whose Accounts were reset (the "Victims") as a result of Change Password Process requests by Company-1 Contractors. Each subscriber informed me that he or she had not asked the Social Media Company to reset his or her Account to the email address provided by the Company-1 Contractor and had not authorized anyone else to reset the password to his or her Account. For example:

a. One victim ("Victim-1") informed me that he lost access to his Service-2 account from on or about July 15, 2021 through on or about July 20, 2021. He regained access after contacting Service-2. Victim-1 further stated that when he regained access to his Service-2 account, he saw that many of his followers and postings had been deleted. From reviewing subscriber records produced by the Social Media Company, I learned that on or about July 15, 2021, an email reset was approved for Victim-1's Service-2 account based on a fraudulent Change Password Process request submitted by another co-conspirator ("CC-5") who was paid by MELBOURNE using cryptocurrency paid by CC-1.

b. Another victim ("Victim-2") informed another FBI agent that he lost access to his Service-2 account – that is, Account-2 – in or about early July 2021, despite using two-factor authentication on that account. Victim-2 further stated that he received a text message that threatened to compromise another social media account that Victim-2 had if Victim-2 attempted to recover his Service-2 account. Approximately one month after losing access, Victim-2 was able to regain access, with help from the Social Media Company, and did not observe any changes to the data in his Service-2 account. As discussed in Paragraph 8(b) above, CC-2 had submitted a Change Password Process request for Account-2 on or about July 2, 2021 that was approved on or about July 7, 2021, for which CC-2 received payment from MELBOURNE that had been paid by CC-1.

11. Based on my review of session logs for the Accounts, I also learned that at least approximately 30 Accounts were accessed from IP addresses that had also been used to access CC-1's Exchange-2 Account. Approximately 18 other Accounts were accessed from other IP addresses assigned to Internet service providers in Turkey, where CC-1 is believed to be located.

12. Finally, based on my communications with representatives of the Social Media Company, I learned that it incurred costs of more than $5,000 in investigating and remediating this account takeover scheme.

WHEREFORE, I respectfully request that arrest warrants be issued for KENDEL ANTHONY MELBOURNE, the defendant, and that he be imprisoned or bailed, as the case may be.

Bryan Demberger (by VF with permission)
BRYAN DEMBERGER
Special Agent
Federal Bureau of Investigation

Sworn to before me by reliable
electronic means this
13 day of May, 2024

THE HONORABLE VALERIE FIGUEREDO
UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF NEW YORK